NAVCIRT Receives SAS Award for Network Defense

By Journalist 2nd Class (SW/AW) Jennifer Zingalie, Naval Network Warfare Command Public Affairs

Information technology gives the warfighter options beyond fighting the enemy on the seas, above the seas or under the seas …

The Navy Computer Incident Response Team (NAVCIRT) received the SAS Enterprise Intelligence Award May 11 in Washington, D.C. The award recognizes achievements in solutions to computer network defense through software application, and illustrates the dedication of NAVCIRT's watch team in preventing virus attacks, intrusions and disruptions to the network that could affect and degrade Navy operations.

SAS, a company that creates business software for analyzing large amounts of data, recognized the strategic vision and collaborative efforts of the NAVCIRT in applying business intelligence to enhance organizational performance.

According to Capt. Steven Carder, NAVCIRT commanding officer, the application of information technology gives the warfighter options beyond fighting the enemy on the seas, above the seas or under the seas.

"We are taking the fight to the enemy in the cyber domain. The tools we use allow us to see where a problem is geographically and, in turn, allow us the capability to provide defense-in-depth and support mission fulfillment at the right time."

"The Department of Defense runs the largest computer network in the world, and our job is to defend the Navy portion of the network. Information is a critical commodity, and it is essential for all the network components to work together to make us an effective warfighting force because any compromise of those components degrades our warfighting capability," said Carder.

"The potential for cyber warfare is very real, and we deal with thousands of probes against DoD perimeter defenses every day," said Carder. "We know that we have enemies with capabilities to wage war in an information domain."

By using the MOBIUS application, watchstanders can provide situational metrics on the status of the network. The software stores cyber security data for historical analysis, trending, data visualization, reporting and event-correlation capabilities that deliver real intelligence on potential threats. The system is based on SAS Intelligence Platform components that include SAS Enterprise BI Server, SAS ETL Server and SAS Intelligence Storage.

MOBIUS is named after the mathematician August Ferdinand Mobius, who devised a two-dimensional surface with only one side.

"The MOBIUS application helps us look for anomalies or indications of warnings of a computer network attack," said Jim Granger, NAVCIRT technical director.

"We look for probing activities, precursors of someone doing reconnaissance for a possible later attack. We can use this information to stop attacks in progress or predict future attacks, and ideally stop them before they start," Granger said.

"In this net-centric era it is important that those in network security are proactive instead of reactive. That is just what we are," said Granger. "We are proud to have tools that can enable us to better do our job monitoring computer networks. We are able to make more informed decisions that drive us forward."

As Granger puts it, NAVCIRT watchstanders are a lot like firefighters. In the old days, a fire in a building would cause one main alarm to sound, but once the fire was put out the entire building would have to be searched to find the source. Eventually, it was decided there needed to be dozens of detectors or sensors everywhere. With these in place, fires were easier to pinpoint, and potential fires could be averted.

Cryptologic Technician (networks) 1st Class Dan Ricci, an assistant watch officer at NAVCIRT, said that "fire prevention" happens every day. "Network security has been happening for awhile; however, there were only a certain amount of sensors placed around the world. Now we have sensors everywhere, and we are able to look at a lot of information at one time," said Ricci.

"We have people who analyze this data. Before, they would have to eyeball long lists of data looking for trends and identifying probes of possible computer threats," said Ricci.

"Now we have software known as MOBIUS that allows us to do our job more efficiently because it gathers similar information and patterns or trends for us; it does the leg work. This allows the analyst more time to look at the data in-depth and respond more rapidly to any threats."

NAVCIRT's cyber warriors are always at general quarters keeping the lines of communication open. "One of the greatest benefits of MOBIUS is that it makes information readily available to the warfighter," said Granger. CHIPS